**AFRL-IF-RS-TR-2006-266**
**Final Technical Report**
**August 2006**


# NATIONAL STRATEGY TO SECURE CYBERSPACE

**DNK LLC**

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED*

**AIR FORCE RESEARCH LABORATORY**
**INFORMATION DIRECTORATE**
**ROME RESEARCH SITE**
**ROME, NEW YORK**

**STINFO FINAL REPORT**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2006-266 has been reviewed and is approved for publication.

APPROVED: /s/

ROBERT L. KAMINSKI
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, Jr.
Technical Advisor, Information Grid Division
Information Directorate

# REPORT DOCUMENTATION PAGE

*Form Approved*
**OMB No. 0704-0188**



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| AUG 2006 | Final | Mar 05 – Jul 06 |

**4. TITLE AND SUBTITLE**

NATIONAL STRATEGY TO SECURE CYBERSPACE

**5a. CONTRACT NUMBER**
FA8750-05-C-0044

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**
N/A

**6. AUTHOR(S)**
Keith T. Schwalm

**5d. PROJECT NUMBER**
DHSA

**5e. TASK NUMBER**
DN

**5f. WORK UNIT NUMBER**
KC

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
DNK LLC
12300 Crested Moss Road, N.E.
Albuquerque NM 87122-4306

**8. PERFORMING ORGANIZATION REPORT NUMBER**
N/A

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

AFRL/IFGA
525 Brooks Rd
Rome NY 13441-4505

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSORING/MONITORING AGENCY REPORT NUMBER**
AFRL-IF-RS-TR-2006-266

**12. DISTRIBUTION AVAILABILITY STATEMENT**
*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 06-575*

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**
The objective of this effort was to coordinate research and development activities throughout private industry, academic laboratories, and private research laboratories to support the development of a national strategy for securing cyberspace. The approach explored the development of cyber technology strategies and programs related to the mission and roles of Homeland Security Advanced Research Projects Agency. Program goals with external clients including IT industry, critical infrastructure sectors, and academics were also explored.

**15. SUBJECT TERMS**
Cyber security,Critical Infrastructure Protection□□

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Robert Kaminski |
| U | U | U | UL | 27 | 19b. TELEPONE NUMBER (*Include area code*) |

# Table of Contents

# Final Report in Support of HSARPA/DHS Activities

## 1 Introduction

This contract was awarded in March, 2005, to DNK LLC for general consulting support of HSARPA/DHS activities as assigned by the Program Manager for Cyber Security, Dr. Douglas Maughan. This support involved participation in the Secure Protocols for the Routing Infrastructure, DNSSEC Deployment Coordination Initiative, and a developing a strategy to raise awareness in Congress.

Monthly reports were provided during this activity detailing the consulting work provided. Included below is a summary of that work and included as attachments in the appendices as needed.

This report will also serve as the monthly report for May 2006; a total of 106 man-hours will be invoiced for this month. To date, 708 man-hours have been invoiced for a total of $199,586.60.

## 2 Activity

This contract only supported two of the activities currently funded by the cyber security portfolio in HSARPA/DHS: Secure Protocols for the Routing Infrastructure and the DNSSEC Deployment Coordination Initiative. There was an additional tasking assigned to DNK LLC by the Program Manager, which along with the other two activities is summarized in the following sub-sections.

### 2.1 Secure Protocols for the Routing Infrastructure (SPRI)

DNK LLC participated in the first two workshops of the Secure Protocol for Routing Infrastructure (SPRI) activity. The initial workshop met in Arlington, VA, and involved participants from government, industry (providers and vendors), and academia discussing the security challenges facing the routing infrastructure. After this initial workshop, DNK LLC provided recommendations made by government and private sector on routing security made since and including *The National Strategy to Secure Cyberspace* (see Appendix A).

The second workshop met in Seattle, WA, and included operators of the routing infrastructure. The operators requested R&D in support of improved open source tools; and, it was collectively agreed that the routing databases need to be cleaned up, with creation of best practices for implementation, as well as training and awareness. DNK LLC was not assigned any action out of this workshop and from this point forward no longer provided support on this activity.

## 2.2 DNSSEC Deployment Coordination Initiative

Participation in this activity was in general support on the deployment of DNSSEC throughout government and private sector. DNK LLC was specifically tasked with developing a relationship with the financial services sector, assistance with the communication plan, and developing a FAQ for the website.

The relationship with the financial services sector was developed through BITS, an association supporting the IT and infrastructure needs of the sector. A series of meetings were held via telephone conference call to introduce a working group of BITS to DNSSEC and then discuss the deployment strategies in their sector. BITS requested a proposal for setting up a test-bed deployment with a couple of institutions (first internal draft for comment is attached as Appendix B). They also requested another technical brief to better understand the deployment impact on manpower and equipment. This activity was left on hold pending work on the government front as requested by the Program Manager.

The working group for this initiative began meeting in monthly October 2005 to develop a communication plan on DNSSEC deployment. After that initial meeting, DNK LLC provided a message development matrix for use in this activity (final version can be found in Appendix C). Specific assignments included providing the DNSSEC recommendation made since and including *The National Strategy to Secure Cyberspace* and FAQ pages already posted on the Internet (Appendix D).

Activity on DNSSEC involves several contractors, each with a specialized task. A FAQ was needed for the activity's website to cover the basics of DNSSEC and the work being done by the contractors. DNK LLC built several versions of a FAQ, the final being a simplified one submitted for publishing on the website. The FAQ, as submitted, is included in Appendix E.

DNK LLC provided other support on this activity. Language was developed for including in legislative language in Congress combatting identity theft and phishing. This legislation was later dropped; the final language as passed to CSIA is included as Appendix F. The Program Manager requested a proposal to understand the economic costs of cyber security, both in preventing it and in response and mitigation to attacks. DNK LLC proposed teaming with the Monitor Group to model these costs, however, funding was not available to proceed. There was also participation as a panelist on the business case for adoption in a workshop on DNSSEC held at the ICANN meeting in Vancouver, BC. Finally, DNK LLC introduced the DNSSEC initiative to the Office of Management and Budget and coordinated the kickoff meeting.

## 2.3 Strategy for Raising Awareness on the Hill

The Program Manager asked for assistance with raising the level of awareness on the hill with regards to cyber security R&D. It was suggested that HSARPA work with an association like the CSIA to get its board members to submit a letter to the Secretary of DHS. Another strategy point would be to gather a letter signed by the "top 100" cyber security experts in the country to the Congress on the lack of attention to HSARPA's

portfolio. Finally, it would be important to learn who the key members of Congress are on the topic of cyber security as communication points.

Key members and staffers:

- Rep. Boehlert (NY) and his staff Elizabeth Grossman and Tim Clancy
- Rep. Lungren (CA) and his staff Rachel Warner
- Rep. Peter King (NY)
- Sen. Smith (ID), specifically on PCS/SCADA issues
- Allison Boyd, Committee on Homeland Security and Governmental Affairs
- Sterling Marchand, Committee on Homeland Security

# 3 Conclusion

Beginning in March 2005, DNK LLC provided general consulting support on various activities for HSARPA/DHS Program Manager Dr. Maughan. This consulting was provided for activities in response to *The National Strategy to Secure Cyberspace*, released by President Bush in February, 2003. A monthly report was provided throughout the activity on this contract describing the activity for the month and number of man-hours invoiced during that same period. This final report will serve as the monthly report for May 2006 where a total of 106 man-hours will be invoiced. Activities during May included delivery of the DNSSEC FAQ for the web-site, review of the DNSSEC Newsletter, and preparation of this final report.

# Appendix A

## Recommendations on Routing Security

The following were extracted from the major activities since and including *The National Strategy to Secure Cyberspace*. Citations are included at the end of each entry. There is no order to their appearance.

Hardening the Internet - Best practices should be developed for filtering access to the management and control planes of routing devices, and that education and outreach be done in this area. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 5

Network Operations - The routers/switches that comprise a network should have strict filtering placed on the entry ports (VTYs, Console, AUX) of the device. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 10

BGP - encourage ISPs to perform ingress route filtering from their customers. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 2

BGP - encourage ISPs to increase the geographic diversity and number of peering connections. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 2

BGP - ISPs should implement route dampening in accordance with RIPE Routing Working Group Memo 229 to reduce disruptions of BGP peering due to rapid changes in routing information by a BGP peer. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 2

BGP - ISPs should implement maximum prefix limits on peering interconnects to limit their exposure to accidental or intentional route de-aggregation. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

BGP - encourage the use of MD5 encryption on BGP4 TCP links. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

BGP - the government should fund research to move the routing (and DNS) databases to strongly authenticated systems with accurate data. This is a prerequisite for many future verification and authentication systems. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

BGP - simply using IPsec on the BGP sessions between peers should be considered prior to implementing Secure BGP. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

BGP - complete the research and development work on Secure BGP. Test the implementation in a real Internet environment, or in a test bed environment such as Internet 2

or a more appropriate test bed, to determine if it is operationally practical and effective in solving the significant BGP security issues. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

BGP - ISPs should investigate the feasibility of egress route filtering at major peering points. This is an area that more research and testing are needed. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

BGP - to counter Distributed Denial of Service attacks on peering routers, it is recommended that these routers implement counter measures against DOS attacks. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3

Hardening the Internet - Operators, government, and enterprise should work to configure their networks so that access to the management planes of their routing devices goes out-of-band from the main data paths/network. Investigate possible filtering and interconnection architectures for routing devices to determine techniques that can physically and/or logically separate user traffic from control and management plane traffic be applied where appropriate. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 5

Hardening the Internet - Secure the machines that control login, monitoring, authentication, and logging to/from routing and monitoring devices. administrative and operational control of the authentication infrastructure needs to be distinct from that of the routing infrastructure, or logging related to malicious or accidental misconfigurations can be too easily erased. Implement change control systems that at a minimum log all configuration changes of all routing devices. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 6

Hardening the Internet - Investigate the feasibility of having separate out-of-band channels (either physical or virtual) for exchange of routing and other control-plane information between routing devices, where possible. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 8

Hardening the Internet - Longer-term investigation should be done to ensure that data center and overlay network operators are protecting their infrastructure of routing, switching, and computing devices properly. Formal relationships should be established and strengthened between colocation and overlay network operators so that government NOCs can have communication with, and visibility into, those infrastructures. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 8

Hardening the Internet - Source address filtering should be implemented across the Internet as soon as feasible – hopefully with substantial progress made in 2002. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 8

DHS, in coordination with the Commerce Department and appropriate agencies, will coordinate public-private partnerships to encourage: (1) the adoption of improved security protocols; (2) the development of more secure router technology; and, (3) the adoption

by ISPs of a “code of good conduct,” including cyber security practices and security related cooperation. The National Strategy to Secure Cyberspace A/R 2-4

When required by law, Network Operators and Service Providers should have procedures in place to support wire taps for court orders, or for other appropriate reasons (e.g., property rights protection from harmful activity). Network Operators and Service Providers should have procedures in place to identify and respond to harmful actions or traffic being routed through their network. NRIC V Focus Group 2 Subcommittee 2.A, pg. 67

In order to maintain a stable IP service and/or transport, the volatility of route advertisements must be managed. Procedures and systems to manage and control route flapping at the network edge should be implemented. NRIC V Focus Group 2 Subcommittee 2.A, pg. 68

Critical Network Elements (e.g., Domain Name Servers, Signaling Servers) that are essential for network connectivity and subscriber service, need by design and practice to be managed as critical systems (e.g., secure, redundant, alternative routing); and, should store multiple software versions and be able to fallback to an earlier version. NRIC V Focus Group 2 Subcommittee 2.A, pg. 68 & 70

Service Providers and Network Operators should have a route policy that is available as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting. NRIC V Focus Group 2 Subcommittee 2.A, pg. 69

Criteria should be established by each Service Provider to ensure that all new hardware (e.g., routers, switches, call servers, signaling servers) meets a mutually agreed upon reliability threshold before it is brought into service on the network. NRIC V Focus Group 2 Subcommittee 2.A, pg. 86

Routing controls should be implemented and managed to prevent routing conditions such as infinite looping, flooding of datagrams across data networks, and other conditions as addressed in RFC 1918 (RFC 1918 is available via http://www.ietf.org/rfc/rfc1918.txt). Routing controls should be implemented across network boundaries to throttle flooding. NRIC V Focus Group 2 Subcommittee 2.A, pg. 86

Identify critical routes and provide these routes with additional protection. (Not sure what "routes" are - might want to look up.) NRIC V Focus Group 2 Subcommittee 2.A, pg. 92

Provide physical diversity on critical routes when justified by a thorough risk/value analysis. NRIC V Focus Group 2 Subcommittee 2.A, pg. 92

Hardening the Internet - Vendors, in cooperation with operators, government, and enterprise, should work to ensure that effective filtering and rate-limiting is implemented to protect router CPUs (the "control plane"). It is important to coordinate the implementation of such protections in the forwarding plane (on the line cards) so that such filtering can be done at wire speed. NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 7

Service Providers should operate a route database. That database should provide the routing advertisement source from the Network Operator's perspective. The database should be accessible by peers, customers and other users. NRIC V Focus Group 2 Subcommittee 2.A, pg. 69

Service Providers should operate a route registry database of all the routes advertised by their network with the source of that advertisement. NRIC V Focus Group 2 Subcommittee 2.A, pg. 69

# Appendix B

## DNSSEC Pre-Operational Experiment

## 1 Motivation and Rational

The security extensions to the DNS protocol are progressing through the standards bodies. One protocol extension in particular, DNSSEC, is mature enough for deployment. While there has been some operational testing of DNSSEC, there needs to be more, and it needs to focus on using actual zone operators and actual zone data for two specific reasons: operational experience and operational feedback.

Involving actual zone operators in the testing will permit them to gain "near real-world" experience with the operational use of DNSSEC. This experience would allow operators to fully deploy DNSSEC with more confidence and in a shorter time-period when the organization fields DNSSEC operationally.

This experiment will involve participation from two primary sources. The Department of Homeland Security (DHS) Science and Technology Homeland Security Advanced Research Projects Agency (HSARPA) will provide XX funding to offset the costs and YY materials and personnel. The members of BITS will be provide ZZ materials and personnel.

## 2 Objectives

This experiment will develop and operate an environment that will permit the use of DNSSEC on copies of several operational zones without impacting the functioning of the actual operational zones. Actual zone operators will perform the operation of the environment.

We call this environment a "Shadow DNS" and the specific zones that are part of the experiment "shadow zones." Even though the "shadow zones" are part if the normal DNS hierarchy, it is anticipated that no "operational functions" will be associated with the "Shadow DNS." Using this shadow environment prevents any unexpected or unknown problems from affecting the actual operational zones while still offering the actual zone operators participating near real-world experience in the operational use of DNSSEC. We refer to the currently operational zones that are as simply the "real zones."

Involving operators will also allow them to give feedback to engineering, development, and standards bodies on the impact of DNSSEC on their operations. Feedback from actual operators will be invaluable to everyone involved in developing DNSSEC.

Additionally, testing DNSSEC with actual zone operators and actual zone data is intended to expose any unexpected or unknown problems that would be encountered during operational deployment in a safe, non-operational environment. If problems are identified in the experiment, they can be resolved prior to deploying DNSSEC.

Finally, testing DNSSEC will allow for validating the interoperability of different DNS sever implementations, including at least ISC BIND version 9 and commercial Nominum name servers, which should minimize deployment risks and possibly assist in identifying any limitations or required management interactions.

## 2.1 Outcomes

This experiment is expected to include the full set of technical and operational functions needed for the operation of DNS Secured zones. The experiment will develop methods for secure signing of zone data as well as secure transfer of the signed zone data to the primary name server. The experiment will also provide experience to further develop guidelines for signature expiration and key rollover.

To gain the most insight into the operational impact of DNSSEC, changes made to the real zones will also be made to the shadow zones. Due to the inclusion of multiple zones operated by different organizations, this continual updating will provide considerable information about the amount and type of inter-organizational coordination needed during actual deployment and provide operators with the opportunity to use existing and emerging tools for managing signed DNS zones.

The experiment will determine procedures that must be followed when a new zone is added to the hierarchy, including:

- How the new zone information is provided to the parent zone.
- The authentication mechanisms used during communication between the operator of the child zone and the operator of the parent zone.
- A secure channel used by the operators to exchange zone information, including DS records.

The experiment will also determine the set of tools needed to help operators manage their secured zones. These tools will be used for zone signing, key management, and key rollover.

The following questions are examples of the outcomes the experiment hopes to obtain.

- After the initial configuration, is the zone properly secured?
  - Are the answers returned from queries to the name servers correctly signed?
- After changes to the zone are made, is the zone still properly secured?
  - Again, are answers returned from queries to the name servers correctly signed?
- Are the procedures for signing zones and participating in a secure hierarchy reasonable?
  - Are operators able to follow the procedures? Do they make sense? Are they too difficult?

# 3 Approach

This experiment will establish a set of shadow zones that contain the data from the real zones. DNSSEC will then be applied to the shadow zones. In all other aspects, including operation, the shadow zones are intended to be as close to the real zones as is practical. Separate name servers

from the operational name servers will serve the shadow zones. We expect that the name servers for the shadow zones will be operated in the same manner and largely by the same people that operate the real zones with the addition of any functions necessary to support DNSSEC in the shadow zone.

The experiment will create a new hierarchy underneath real zone (which currently exists). This new hierarchy will be a delegation from the real zone but will be a shadow zone of the real zone and will be operated as if it is the real zone. DNSSEC will be deployed within this shadow hierarchy. To illustrate, if the real zone is example.com the shadow zone might be test.example.com and test.example.com would contain essentially the same data as example.com. The two notable differences in zone data between example.com and test.example.com are 1) the information in example.com for the delegation of test and 2) the information for test.example.com name servers would likely differ.

The experiment will include at least two shadow zones. One described above will shadow a real zone (e.g., test.example.com) and another will shadow a delegation of example.com, e.g. labs.example.com (real zone) will be shadowed by labs.test.example.com. To gain the greatest benefit from the experiment, the delegation (e.g., labs.example.com) will be operated by a different set of people than those that operate the parent zone (e.g., example.com). The experiment should also include operational personnel associated with the zones that control the content of the DNS data for the real zones. In some but not all instances, the people that control the content may be different than the people that operate the name servers for the zones and should also participate in the experiment.

As discussed before, changes made to the real zones will also be made to the shadow zones, i.e., the shadow zones will be kept in-sync with the real zones as the experiment progresses.

To ensure the greatest participation from operational personnel, the primary name server for each shadow zone will be located in the same facility as the operators of the real zones. There should also be two secondary name servers for each shadow zone, which may initially be located in the same facility as the name server for the real zones. These secondary name servers should be moved to some other facility by the end of the experiment so that geographic diversity of name servers can be tested. Some of the secondary name servers may provide secondary service for multiple zones. Additionally, the experiment will use TSIG between the primary and secondary name servers to ensure that zone transfers are secure.

## 3.1 Testing

The experiment will use various methods to test whether the zone operations are proceeding correctly. One of these methods will include querying the name servers involved in the experiment from other machines on the network. These queries will be sent using the command line tool dig that is part of the BIND distribution.

## 3.2 Recursive Server Separation

The experiment will also test the separation of recursive name servers from authoritative name servers. Current best operating practices requires that recursive name servers must be physically separate from authoritative name servers. The configuration and operation of the recursive servers needs to be determined.

## 3.3 Shadow Zone Setup

In order to set up the shadow zones, there are a number of necessary components. In all likelihood, the experiment will be performed in stages.

Initially, the operators of each of the shadow zones will identify the equipment and network connection facilities for the shadow zone name servers. In the initial phase, all of the name servers may be located in the same facility as the real zone name servers but planning for later stages needs to include having secondary name servers for the shadow zones in other (non-collocated) facilities. Also, the initial stage needs to include establishing the delegation of the shadow zone from the real zone as well as establishing the delegations from the shadow zone. Each of the zone operators needs to make copies (with required adjustments) of data from the real zones for use in the shadow zones.

## 3.4 Software

The software for the experiment will generally be the same as what would be in place for the real zones if they were fielding DNSSEC at the time of the experiment.

- Name Server Software: ISC BIND
  - The current name servers for the real zones frequently run ISC BIND as the name server software. The current DNSSEC extensions that the experiment will test are only provided by BIND version 9.3 and later. The experiment will use the most current version of BIND 9.3 at the time the name servers are being configured.

Additionally, there are several tools that could assist DNS operators with managing secure zones.

- DNSSEC Tools
  - URL: http://www.dnssec-tools.org
  - Set of tools for managing DNS secured zones and DNSSEC aware applications
- Nominum Foundation
  - URL: http://www.nominum.com
  - Caching Name Server
  - Authoritative Name Server
  - Dynamic Configuration Server
  - At this point, the amount and type of Nominum software in the experiment has not yet been determined.
- Infoblox
  - URL: http://www.infoblox.com

    - DNS Server Appliances
- Olaf Kolkman's DNSSEC Extensions to Net::DNS, Net::DNS::SEC
    - URL: http://www.ripe.net/disi/
    - A set of Perl tools for DNS administration.
- Shinkuro
    - URL: http://www.shinkuro.com
- A file sharing system that allows users to securely share files with other users.
    - Could be used to send DNS information, such as DS records, to a parent.
    - Shares files via behind-the-scenes email messages.
    - It only runs on Microsoft operating systems, so would require another box to use it.

# 4 Cost and Requirements

Based on the above software and hardware suggestions, the cost for equipment would be $$$. In terms of manpower, it is estimated that the experiment would require HH man-hours from each participating organization.

# 5 References

The following documents are listed for informational purposes. Each of the documents contains information that might be useful for the experiment and might even be improved from lessons learned during the course of the experiment.

"NIST guide 800-81 "Secure Domain Name System (DNS) Deployment Guide""
http://csrc.nist.gov/publications/drafts.html#sp800-81

http://www.dnssec-deployment.org/

http://www.dnssec.net/

http://www.nlnetlabs.nl/dnssec/

http://www.ripe.net/disi/

Papers from the 5th USENIX UNIX Security Symposium, Salt Lake City, Utah, June 1995

P. Vixie: DNS and BIND Security Issues

http://www.usenix.org/publications/library/proceedings/security95/vixie.html

S. Bellovin: Using the DNS for Break-ins

http://www.usenix.org/publications/library/proceedings/security95/bellovin.html

Appendix C

# DNSSEC Message Development

| | Audience Goals | + Drivers | + Barriers | → Messages |
|---|---|---|---|---|
| **Internet Community** | • DNSSEC awareness, implementation, adoption, and road map<br>• Assign personnel to implement DNSSEC<br>• Name DNSSEC a "best practice"<br>• Request speakers on DNSSEC | • ***DNS threats*** / security of Internet infrastructure<br>• ***Trust issues*** with customers re: security of internet | • Ownership of DNSSEC keys and registration<br>• "***So what?" / lack of awareness***<br>• Technical requirements not clear<br>• Trust in government's intentions<br>• ***No clear business case / ROI issues*** | |
| **Private Sector** | • DNSSEC awareness, implementation, adoption, and road map<br>• Assign personnel to implement DNSSEC<br>• Name DNSSEC a "best practice"<br>• Request speakers on DNSSEC<br>• Vendors create secondary DNSSEC info market | • ***DNS threats*** / security of Internet infrastructure<br>• ***Trust issues*** with a) customers and other users re: security of corporate networks and personal data and b) other businesses<br>• Regulatory requirements | • No apps DNSSEC aware (yet)<br>• Ownership of DNSSEC keys and registration<br>• "***So what?" / lack of awareness***<br>• Technical requirements not clear<br>• Trust in government's intentions<br>• ***No clear business case / ROI issues*** | |
| **Public Sector / Int'l Community** | • Develop policy on DNSSEC adoption and best practice guides<br>• DNSSEC awareness, implementation, adoption, and road map (including int'l)<br>• Task specific officials with achieving DNS security<br>• CIO groups name DNSSEC "best practice"<br>• Establish federal, state, and local coalitions on DNS security | • Regulatory requirements (FISMA, OMB etc)<br>• Leader and driver on cyber security<br>• National Strategy to Secure Cyberspace recommendation | • No apps DNSSEC aware (yet)<br>• Ownership of DNSSEC keys and registration<br>• "***So what?" / lack of awareness***<br>• Technical requirements not clear<br>• Process across TLDs not clear<br>• ***No clear business case / ROI issues*** | |
| **Consumers / End Users** | • Separate awareness campaign<br>• After companies begin adopting DNSSEC measures, consumers ask for DNS security<br>• Understanding who you are submitting data to (addressing)<br>• Understand DNSSEC will not break the Internet and no action required | • ***Trust issues*** with security of personal data handled by private and public sector entities (i..e, Who are you exchanging data with?) | • No apps DNSSEC aware (yet)<br>• Ignorance of DNSSEC issues<br>• Apathy | |
| **Media** | • Accurate media coverage that includes DNSSEC initiative's viewpoint and information<br>• Separate awareness campaign<br>• Understanding who you are submitting data to (addressing)<br>• Understand DNSSEC will not break the Internet and no action required by users | • ***Privacy / Trust headlines:*** hot topic with audiences | • No crisis event to date / no "story"<br>• "***So what?" / lack of awareness***<br>• Trust in government's intentions<br>• ***No clear business case / ROI issues*** | |

# Appendix D

Recommendations made since and including the *National Strategy to Secure Cyberspace* related to securing DNS:

- DNS - encourage physical diversity for top-level domain servers.
- DNS - encourage greater software diversity for DNS server systems.
- DNS - IETF DNS Extension Working Group should complete the specification of DNSSEC.
- DNS - the government should fund the completion of DNSSEC.
- DNS - operators of routing registries, ISPs and operators of large DNS zones to experiment with the DNSSEC implementation as soon as possible.
- DNS - DNS server operators to develop disaster recovery and business continuity plans.
- DNS - stronger mechanisms are needed to ensure the authentication of the DNS database along with changes to the database.
    - (NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 2)
- BGP - the government should fund research to move the routing (and DNS) databases to strongly authenticated systems with accurate data. This is a prerequisite for many future verification and authentication systems.
    - (NSTAC Internet Service Provider Working Groups, May 1, 2002, pg. 3)
- The Director of OSTP will coordinate the development, and update on an annual basis, a federal government research and development agenda that includes near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research for Fiscal Year 2004 and beyond. Existing priorities include, among others, intrusion detection, Internet infrastructure security (including protocols such as BGP and DNS), application security, DoS, communications security (including SCADA system encryption and authentication), high-assurance systems, and secure system composition.
    - (The National Strategy to Secure Cyberspace A/R 2-11)

The FAQ pages found dealing with DNSSEC can be found at:

- Nominet DNSSEC Testbed FAQ
    - http://www.nominet.org.uk/TagHolders/Dnssec/DnssecFaq/

- Registrar for .org DNSSEC FAQ
  - http://www.pir.org/RegistrarResources/RegistrarFAQsDNSSecurity.aspx
- Nominum, Inc. DNSSEC FAQs (lot of sites reference this one, including the NL)
  - http://www.nominum.com/getOpenSourceResource.php?id=8
- Verisign Labs DNSSEC Pilot FAQ
  - http://www.dnssec.verisignlabs.com/website/faq.htm
- Verisign Labs DNSSEC Hosting FAQ
  - http://www.dnssec.verisignlabs.com/website/faq.htm
- Internet Society DNS Root Name Servers FAQ
  - http://www.isoc.org/briefings/020/

# Appendix E

## DNSSEC Deployment Initiative Website FAQ

DNSSEC Deployment Coordination Initiative FAQ

1. What is DNSSEC?
2. Why is the Department of Homeland Security working on DNSSEC?
3. Who is involved in DNSSEC Deployment Coordination Initiative?
4. What is the road map?
5. What software is available?
6. What is the current status of the government standards activity?
7. What have been the activities of the DNSSEC Deployment Coordination Initiative?
8. Does DNSSEC secure my Internet communications?
9. How does DNSSEC work to protect my DNS queries?
10. What is the cost of deploying DNSSEC?
11. Where can I learn more about DNSSEC?

1. What is DNSSEC?

DNSSEC is the standard IETF protocol for securing the Domain Name System (DNS). DNS is the process of obtaining an IP number for a specific domain name. When a computer system asks wants to visit a particular website, or send email to a particular site, DNS is used to determine where on the Internet the site is. DNS is like a telephone book that references a IP number to a name. So when a computer wants to address dhs.gov a query is passed to a DNS server requesting the IP number for dhs.gov. The response is then used to communicate directly with that site.

DNS on the Internet is really a collection of many servers. They each hold tables of domain names and assigned IP numbers. The system works on a query response system and the first response is accepted and all others dropped. So a threat to DNS is the ability for a nefarious actor to answer with a false response before the true information is received.

DNSSEC is an extension to the existing DNS systems so that queries are responded to with authenticated information. "All [responses] in DNSSEC are digitally signed. By checking the signature, a DNS resolver is able to check whether the information is identical (correct and complete) to the information on the authoritative DNS server." [Source Registrar Resources]

2. Why is the Department of Homeland Security working on DNSSEC?

In 2003 President Bush released The National Strategy to Secure Cyberspace, which made several recommendations. Recommendation A/R 2-11 stated:

> *The Director of OSTP will coordinate the development, and update on an annual basis, a federal government research and development agenda that includes near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research for Fiscal Year 2004 and beyond. Existing priorities include, among others, intrusion detection, Internet infrastructure security (including protocols such as BGP and DNS), application security, DoS, communications security (including SCADA system encryption and authentication), high-assurance systems, and secure system composition.*

Since the release of the Strategy, the Department of Homeland Security (DHS) has become the lead for cyber security issues and the Science and Technology Directorate within DHS has a portfolio specifically for research, development, testing and evaluation of cyber security activities. Securing DNS was a recommendation in the Strategy and DHS is supporting the progress on that recommendation through the DNSSEC activity. Securing DNS was a recommendation in the Strategy and DHS is furthering progress on that recommendation by supporting the DNSSEC Deployment Coordination Initiative.

3. Who is involved in DNSSEC Deployment Coordination Initiative?

There are three primary contractors: Shinkuro, Sparta and NIST. They are working on road map development and execution (involving international partners), software tool development, Internet standards activity, measurement and evaluation tools, and government and standards activities.

The DNSSEC Deployment Initiative works to encourage all sectors to voluntarily adopt security measures that will improve security of the Internet's naming infrastructure, as part of a global, cooperative effort that involves many nations and organizations in the public and private sectors. DHS Science and Technology provides support for coordination of the initiative.

4. This site has a DNSSEC Deployment RoadMap, what is the road map?

This document was created through the second half of 2004, and released in early 2005. This document describes the basic goal for deployment; the current state of practice, gaps and barriers; a set of sequences and dependencies; and next steps. Its primary audience consists of operators and administrators of the domain name system

(DNS), their vendors and suppliers, and their customers. Refer to the DNSSEC Deployment Initiative homepage or to the sites listed in answer #11.

5. What software is available related to DNSSEC?

This site has provided a page with an update on the available software tools, sorted by role. There are End-System Administrator and End-User tools, Name Server Administrator tools, Zone Data Administrator tools, Zone Contact tools, and Application Developer tools.

6. What is the current status of the US Federal government standards activity?

DNSSEC has been proposed as part of a new standard that aims to help federal agencies improve their information technology security and comply with the Federal Information Security Management Act (FISMA) of 2002. A plan for staged deployment of DNSSEC technology within federal IT systems was included in recently released Draft Special Publication 800-53, Revision 1: Recommended Security Controls for Federal Information Systems. NIST 800-53r1 specifies the mandatory minimum security controls necessary to comply with Federal Information Processing Standards (FIPS) required by the FISMA legislation (Federal Information Processing Standard (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems; and FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems).

A recently released NIST Security Guidance document (Draft NIST Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide) provides the technical details and detailed implementation guidance to assist agencies in deploy new DNS security measures with confidence. Agencies will have a year after final publication to meet the requirements.

For more information see the news release and the Federal Information Processing Standard (FIPS) Publications 199, 200, 800-81and 800-53.

7. What have been the activities of the DNSSEC Deployment Coordination Initiative?

- Road map was published in February 2005.
- NIST developed a DNSSEC testbed; there have been numerous deployment pilots in governments around the world.
- The DNSSEC Deployment Coordination Initiative has worked with the US Government (.gov), and operators of .us and .mil zones towards DNSSEC deployment and compliance.
- Members of the deployment coordination initiative and their counterparts participate regularly in a range of workshops, panels and briefings aimed at technical specialists and potential adopters. You can follow these on the Calendar page.

8. Does DNSSEC secure my Internet communications?

No. Although there is encryption technology used in the certificates used to digitally sign the responses, it does not secure the communication between systems. It is used to verify that the DNS response matches that which the authoritative server maintains. It does not guarantee that the information is correct, only that it is as reported by the correct source. If a nefarious actor responds before the authoritative DNS server then the signature would not match and that response could be dropped as not authentic.

9. How does DNSSEC work to protect my DNS queries?

"Currently, a DNS resolver sends a query out to the Internet and then accepts the first response it receives, without question. If a malicious person were to send back an incorrect response (such as an address to a Web site that was really a phishing site), the resolver would use this address until its cache expired. This is referred to as a 'man in the middle attack.'" [Source Registrar Resources]

10. What is the cost of deploying DNSSEC?

It is too soon to determine the total costs of deploying DNSSEC in any size organization. Studies of performance are still in progress and the personnel require to manage DNSSEC, particularly the tasks associated with managing the keys, is determined by the size of your organization. Manpower impact will involve education in the DNSSEC extension and how to sign and maintain keys. The number of people required to manage DNSSEC would be determined by the size of your organization and number of name servers and zones deployed. Hardware and software impact will be minimal if you are operating ISC BIND 9.3.x, NSD, or Nominum Authoritative Name Server (ANS) -- they are currently the name servers that support DNSSEC.

11. Where can I learn more about DNSSEC?

There are some FAQs that already adress in more detail on DNSSEC, some have been quoted about and can be found at:

- Nominet DNSSEC Testbed FAQ
- Registrar for .org DNSSEC FAQ
- Nominum, Inc. DNSSEC FAQs
- Verisign Labs DNSSEC Pilot FAQ
- Verisign Labs DNSSEC Hosting FAQ
- Internet Society DNS Root Name Servers FAQ
- DNSSEC: DNS Security Extensions is a good website to find a lot of reports, papers, and other documents.

- DNSSEC HOWTO: A Tutorial in Disguise by Olaf Kolkman is a great site on how to deploy DNSSEC.
- The NIST DNSSEC Project
- DNSSEC tools

# Appendix F

**Identity Theft Through Internet Domain Name System Poisoning**

## Background

The *National Strategy to Secure Cyberspace* identified securing the Domain Name System (DNS) as one of several vulnerable services critical to the continued operation of the Internet.

DNS is a naming system that maps an Internet Protocol (IP) address to a name that users can use to address communications on the Internet. For example, if a user wanted to browse the Library of Congress web-site, they point their web-browser to www.loc.gov. Their computer first queries a DNS server[2] to learn with the IP of that domain name is; the DNS server would return, invisible to the user, the IP address of 140.147.249.7. That IP number is then used to initiate a communication with the web-server that answers at that number. Systems can move on the Internet and inherit new IP numbers, that added to the millions of optional addressable systems on the Internet makes DNS a vital service for Internet communications.

Should DNS no longer be available, communication on the Internet is still possible but only by using the correct IP number. For most, this would be impossible.

## Threat

1. Criminals capture passwords, account numbers, and other privacy information by covertly redirecting online consumers to counterfeit web sites.

A misuse of DNS to redirect legitimate communications to an counterfeit system is one of the more prominent threats. This is often referred to as “spoofing” and involves tricking a user in to believing they are actually communicating with the legitimate system. Referring back to the Library of Congress example, if the user’s request for DNS information was intercepted or invalid they would then be directed to the wrong site and a different IP address. DNS spoofing and other malicious activity such as DNS hijacking has direct implication on the identity theft, phishing and spam issues present on the Internet today.

## DNS Security Extensions (DNSSEC)

2. U.S. Government funded research has developed a way to security DNS so that such criminal poisoning and redirection could not occur.

---

[2] There is a hierarchy of DNS severs installed throughout the Internet. All ISPs provide a DNS server, most large organizations maintain their own DNS servers, and all of these communicate with 13 key root servers established around the world. All DNS data starts at the root servers and is populated down through the hierarchy. DNS data records can take several hours or even days to update throughout the whole chain. All of this is important to understand the first phase of DNSSEC adoption.

DNS Security Extensions (DNSSEC) is a security solution for DNS, and is ready for adoption and deployment. This protocol has been in development for the last decade and was recently approved by the Internet Engineering Steering Group and is waiting final publication for adoption. The Homeland Security Advanced Research and Projects Agency (HSARPA) at the Department of Homeland Security has funded this activity and is involved in transitioning from research and development to adoption.

Adoption requires deployment at different levels and will be discussed later in the roadmap. DNSSEC adds to the DNS hierarchy cryptographic signatures that support the integrity of DNS queries. The signatures protect against tampering of DNS data at rest in DNS servers and in transit to a requesting system. They do not secure transmission of the data, nor do they make the DNS data secret. Rather the cryptographic signatures provide authentication on the data returned from a DNS server.

**Roadmap**

3. Commercial adoption of DNSSEC would be encouraged by the use of such technology by the U.S. Government.

    - There are some adoptions that need to occur at the DNS core to support the migration of this technology. Once in place, operators and customers can request signing and publishing of DNS data.

    - Operators of key domains need to follow the roadmap steps: sign, serve, distribute public key, and register subordinate domains.

        - For the Federal Government, this would be required of the .mil (Dept. of Defense) and .gov (Commerce Dept.) domains.

        - Critical infrastructure operators would include the .com (Verisign), .net (Verisign) and .us domains.

    - Customers are those that own subordinate domains below the root domains would need to also follow the roadmap steps: sign, serve, distribute public key, and register subordinate zones.

        - Examples in the Federal Government would be house.gov and senate.gov, and policy direction would come through the Office of Management and Budget through the CIO Council.

        - Critical infrastructure owners and operators could include bankofamerica.com and juniper.net; these customers would require support from the root domains (in both examples Verisign as owner of .com and .net root domains).

**Proposed Legislative Language**

A) Federal government information system networks shall utilize a methodology for securing their Domain Name Systems no later than the end of fiscal year 2007. The

Office of Management and Budget shall direct the adoption of the secure system, assisted by the General Services Administration and the Department of Commerce/ National Institute of Standards and Technology.

B) The Department of Homeland Security, the Department of the Treasury and the Department of Commerce will jointly engage in an effort to encourage private sector adoption of secure Domain Name System technology.

**Conclusion**

An ultimate goal for DNSSEC adoption is for all DNS traffic on the Internet to be DNSSEC compliant. This is a very large challenge, and will require many large sectors, including governments, to adopt and require DNSSEC on their own systems. Returning to our Library of Congress example, if DNSSEC were deployed the user's system would request the DNS entry receiving a response signed by a trusted certificate that the answer provided is for the host it claims to be. If the information is invalid, the user would not receive any information and would not be directed to an invalid web-site. A DNSSEC deployment such as this requires the root server for .gov, the user's ISP, and the Library of Congress all to adopt and support DNSSEC.